Active Directory – Replikace, hlavní operační servery, topologie

Operace kdy si doménové řadiče vyměňují informace se nazývá replikace. Dochází k ní tehdy pokud na jenom doménovém řadiči provedeme změnu. Mezi tyto změny patří:

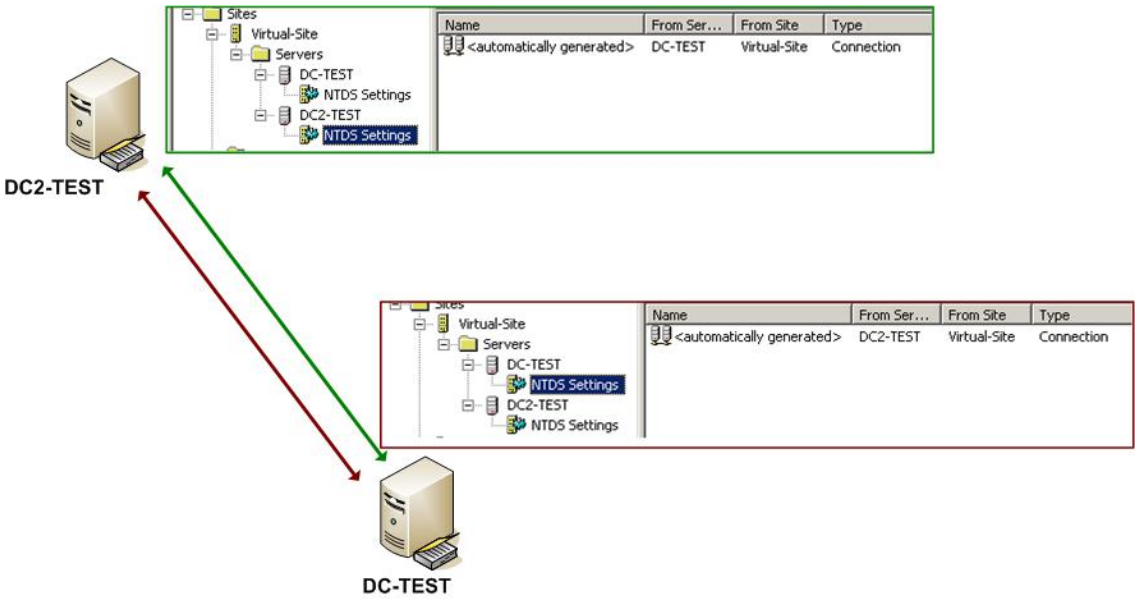
- přidání objektu do AD
- změna některých vlastností objektu (členství ve skupině, telefon apod.)
- přejmenování kontejneru objektů
- smazání objektu

Replikují se buď jednotlivé oddíly Active Directory nebo celá databáze. Způsob replikace závisí na funkční úrovni lesa. Windows 2003 přináší možnost inkrementálních replikací.

Replikační topologie je cesta, kterou putují data v síti, může se lišit pro replikaci schématu, konfigurace, doménového nebo aplikačního oddílu. Pro optimalizaci provozu je možné přiřadit jednomu řadiči několik replikačních partnerů pro různé oddíly Active Directory.

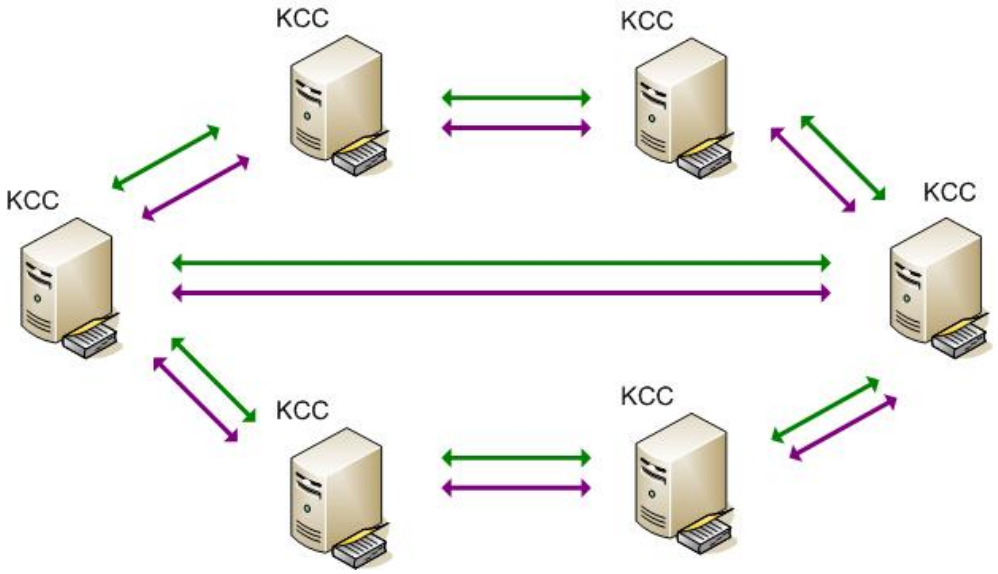
Doménové řadiče, které jsou spojeny pomocí objektů spojení se nazývají **replikační partneři**. Spoje, které propojují replikační partnery jsou **replikační objekty**. Služba, která zajišťuje vytváření replikační topologie se jmenuje **Knowledge Consistency Checker** (KCC). Služba je použita k úpravě replikační topologie pokaždé, když je do domény přidán nový řadič. Je spouštěna v pravidelných intervalech (výchozí hodnota je 15 min). KCC vypočítá nejlepší spojení mezi doménovými řadiči. Pokud dojde k chybě při replikaci v rámci jedné sítě KCC automaticky vytvoří nové spojení mezi řadiči, aby mohly replikace probíhat. Pro kompletní replikaci dat mezi dvěma řadiči domény jsou zapotřebí 2 objekty spojení:

- jeden pro replikaci dat z řadiče A na řadič B, který existuje v objektu NTDS Settings na řadiči B
- a druhý pro replikaci dat z řadiče B na řadič A, který existuje v objektu NTDS Settings na řadiči A



Objekty spojení na řadičích domény

Replikace, které probíhají v rámci jedné lokality se nazývají **Intra-Site** replikace. Tyto výměny informací probíhají často na základě změny v Active Directory. Nepoužívají komprimaci dat.

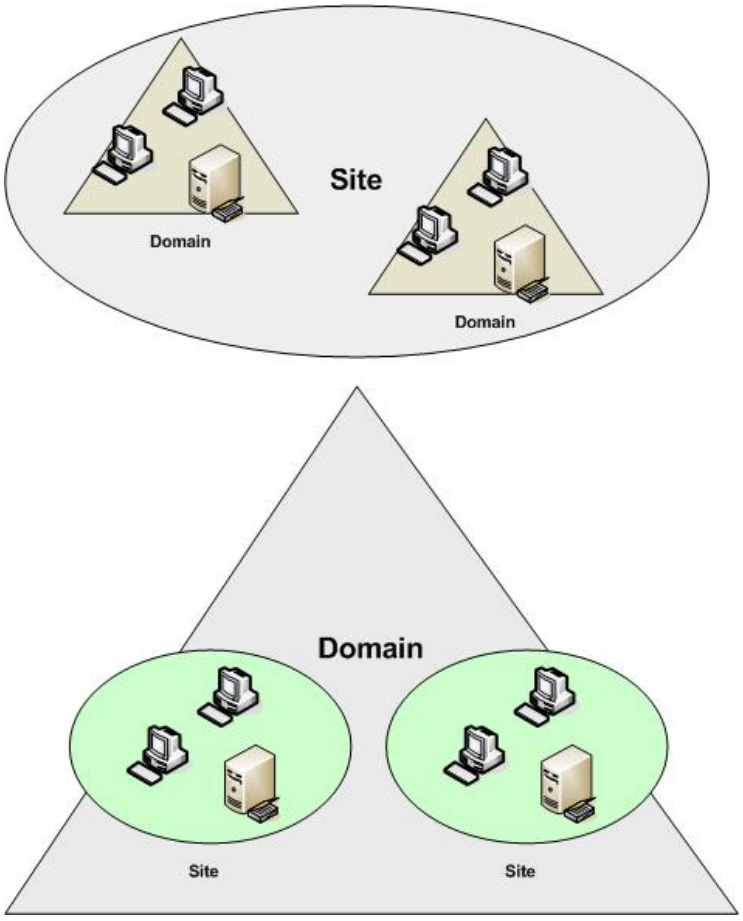


Replikace v rámci jedné lokality

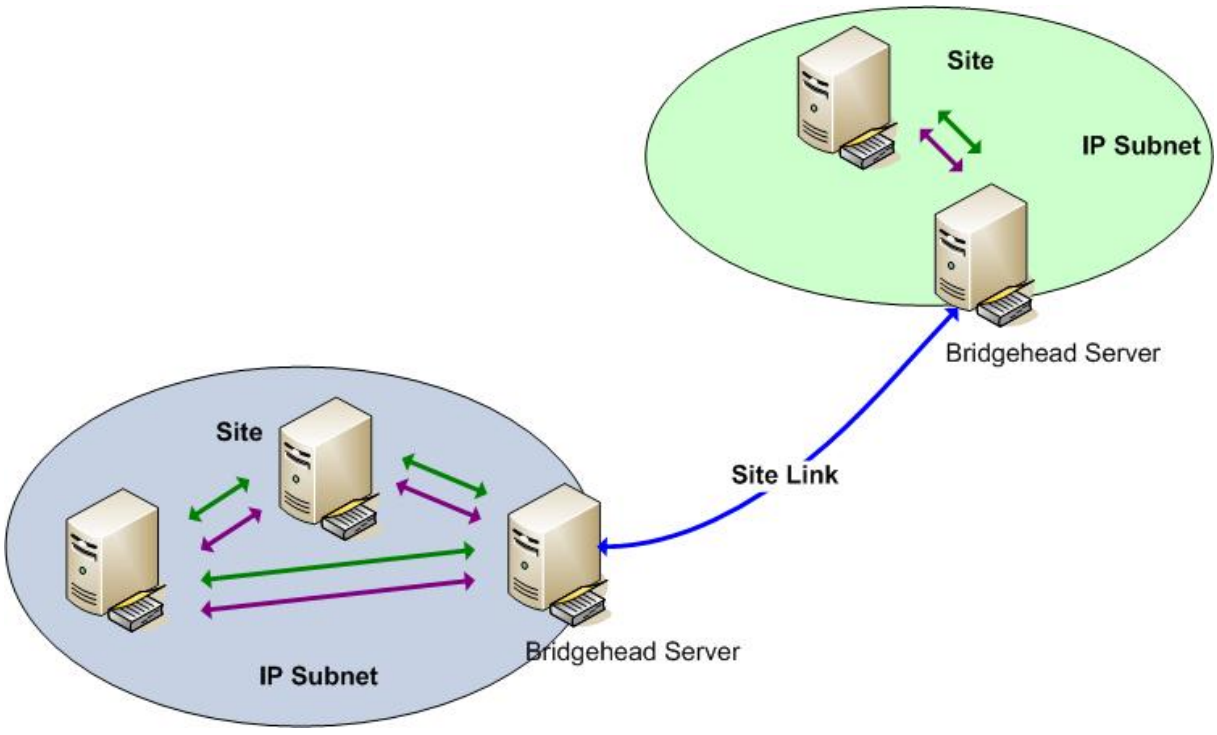
Pokud chceme definovat vlastní topologii replikace tak objekty spojení lze vytvářet i ručně. Toto nemá příliš velký význam v rámci inter-site replikací, ale je vhodné topologii replikací upravovat mezi jednotlivými lokalitami.

V případě rozsáhlejších struktur Active Directory je zapotřebí definovat i replikace mezi lokalitami - **Inter-Site**. Jestliže počítače v rámci jedné sítě jsou spojeny rychlou sítí typu ethernet, tak jednotlivé lokality jsou většinou propojeny pomocí sítě WAN s omezenou rychlostí. U sítí typu WAN také musíme počítat s výpadky, jelikož se jedná o pronajaté okruhy. Jejich provoz nemůžeme většinou ovlivnit. Kapacita linek WAN je také obvykle plánována s ohledem na aplikace důležité pro činnost organizace. Z tohoto důvodu inter-site replikace probíhají podle definovaného plánu a využívají komprimaci dat.
Postup při konfiguraci inter-site replikací by měl být následující:

- definice lokalit (site)
- definice podsítí (subnets)
- přiřazení podsítí k jednotlivým lokalitám
- definice spojení mezi jednotlivými lokalitami (site-links)
- přesun serverů do daných lokalit



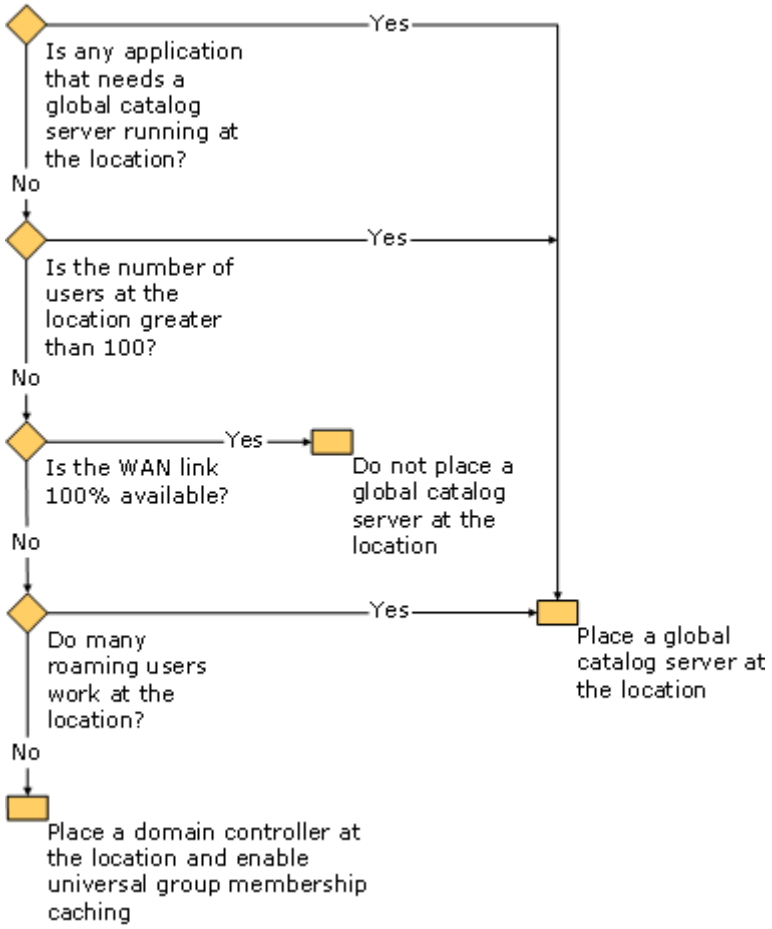
V rámci jedné lokality může být více domén nebo jedna doména může být v několika lokalitách.



Replikace mezi lokalitami využívá objekty Site-Link

Umístění globálního katalogu

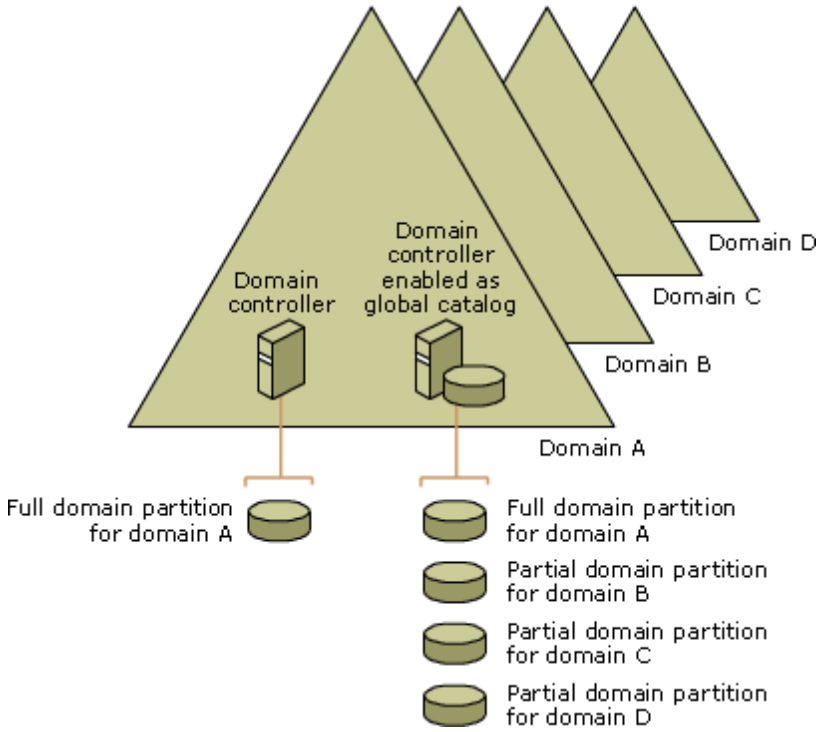
V případě, že máme jednu doménu s jedním řadičem, tak tento doménový řadič hostuje všechny FSMO role a je zároveň globálním katalogem. V případě, že je struktura Active Directory rozsáhlejší musíme umístění FSMO rolí a globálního katalogu určit. Umístění globálního katalogu je důležité i z pohledu replikací, protože příliš mnoho globálních katalogů zbytečně zatěžuje síť. Pro umístění globálního katalogu platí následující pravidla:



Umístění globálního katalogu

Globální katalog je velmi důležitý pro přihlašování do sítě. Nezbytný je zejména pokud používáme univerzální skupiny a v jedné lokalitě se připojují uživatelé z různých domén. V případě, že nemůžeme do dané lokality umístit globální katalog (pomalá linka, omezené prostředky atd.) můžeme na lokalitě aktivovat **universal group membership caching**.

Globální katalog obsahuje oddíly schématu a konfigurace. Domain partition pro doménu, které je členem a částečné doménové oddíly z ostatních domén v lese, které jsou pouze pro čtení. Počítače v síti lokalizují globální katalog pomocí služby DNS.



Obsah globálního katalogu

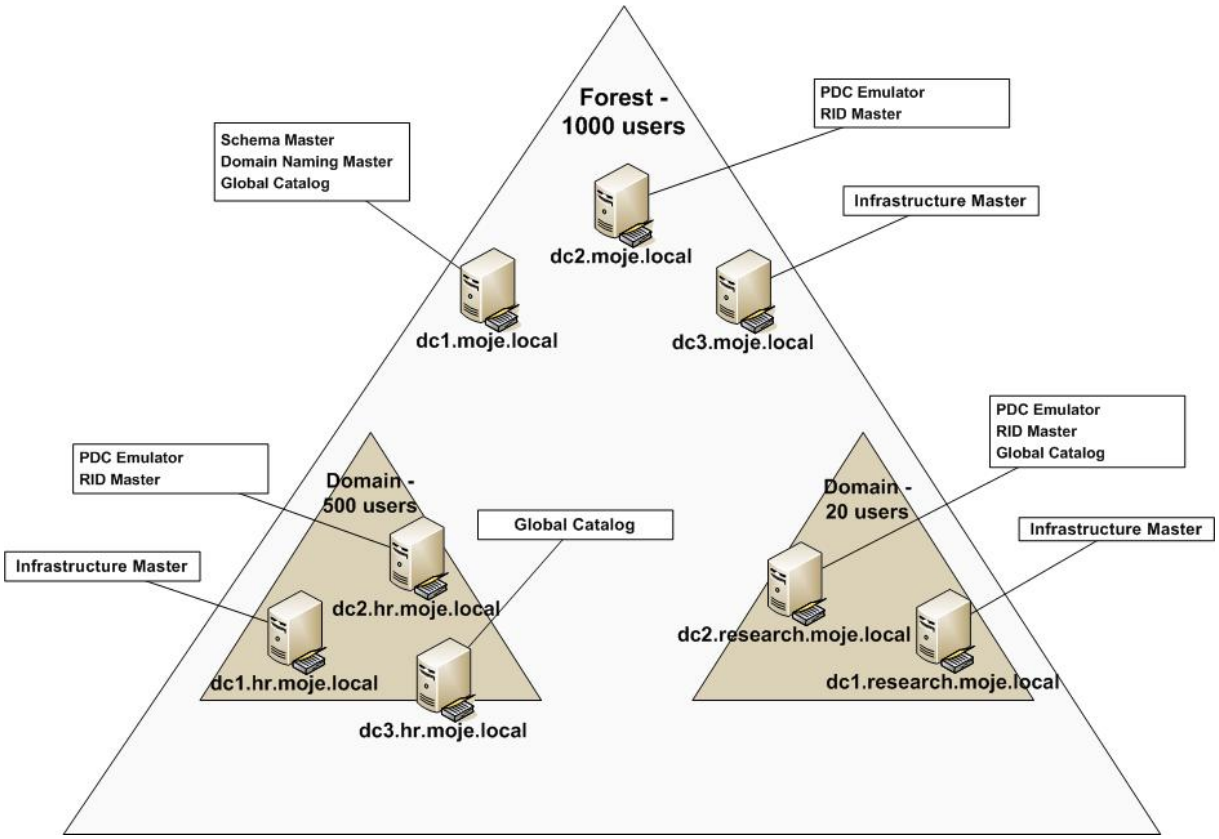
Umístění hlavních operačních serverů

V zásadě je možné postupovat podle následujících pravidel:

- **Schema Master a Domain Naming Master** by měly být umístěny v kořenové doméně na jednom serveru, který by měl být globálním katalogem. V případě, že tyto dvě FSMO role nehostuje jeden stroj je zapotřebí zajistit, aby byly přímými replikačními partnery.

- **PDC Emulátor a RID Master** musí být v každé doméně,jelikož jsou tyto servery často využívány není vhodné, aby tento řadič domény zároveň obsahoval globální katalog. Globální katalogy a PDC Emulátor jsou nejvytíženější řadiče ve struktuře Active Directory. Rozdělením těchto rolí můžeme lépe balancovat výkon.

- **Infrastructure Master** nesmí být na řadiči domény, která obsahuje globální katalog. Toto pravidlo neplatí pouze v případě, že máme pouze jednu doménu nebo naopak všechny řadiče v lese jsou zároveň globálními katalogy.



Umístění hlavních operačních serverů ve struktuře Active Directory